CITY OF SAN ANTONIO

Administrative Directive	**7.5a Establishing IT-Related Directives**
Procedural Guidelines	Guidelines to implement and enforce Citywide IT-related directives and standards.
Department/Division	Information Technology Services Department (ITSD)
Effective Date	June 01, 2013
Revisions Date(s)	December 14, 2017
Review Date	April 2, 2021
Owner	Patsy Boozer, CSO

Purpose

This Administrative Directive (AD) establishes a framework for the City of San Antonio's (COSA) information security program and process for creating or updating and communicating City-administered information technology (IT) system – related directives, standards and procedures. It establishes and identifies responsibilities to help ensure the confidentiality, integrity and availability of City system(s). This directive supersedes 7.8.1 Information Security Program and 7.5a dated December 23, 2008.

The COSA information security program is a framework based on the National Institute of Standards of Technology (NIST) and industry best practices to help maintain the confidentiality, integrity and availability of COSA systems and meet applicable federal, state, and municipal laws, administrative codes, regulations, and/or statutes that apply to City assets. In order to implement COSA IT-related ADs, ITSD will need to develop, update and communicate standards and/or procedures designed to provide reasonable assurance that risk-based system and application security controls and/or countermeasures are commensurate with the value of the asset(s) they protect.

Note: This information security program and its subset of directives, policies, standards and/or procedures are superseded by applicable federal, state, and municipal laws, administrative codes, regulations, and/or statutes that apply to City assets.

Policy

Adherence to this directive will help reasonably assure the security of City assets.

- The Information Technology Services Department (ITSD) has primary responsibility for the security management program and the security of the City's electronic systems. ITSD will establish administrative directives, standards and/or policies to help ensure the security of City system(s)
- Organizational responsibility for the development, implementation, maintenance and/or compliance monitoring of this directive is placed with ITSD
- ITSD will maintain the security management program and monitor its compliance
- COSA is required to protect public assets and resources and it has an obligation to manage information technology systems to comply with Chapter 552 of the Texas

Public Information Act (open public records), Sections 7.71-7.79 of the Texas Administrative Code and 205.001-205.009 of the Local Government Code among other regulations

- All information created, processed, or stored in City-provided information technology systems are the property of COSA
- IT-related Standards may include specifications for acceptable hardware, acceptable versions of software, and acceptable performance of technology, service level agreements, and other categories

This directive applies to:

- All information technology systems, procured with City funds, and/or used in the conduct of City business
- All electronic messaging, equipment and/or technology that are owned or administered by the City including City-owned computers, mobile devices and personal devices reimbursed through COSA stipends (*A.D. 7.9*) are included within the scope of this Directive
- All software, information system(s) and/or other documents developed by City personnel with City funds or licensed to the City of San Antonio
- All data processed, stored and/or transmitted by any City Information Technology System(s)
- All devices that use the COSA network including any "Bring Your Own Device" (BYOD)
- All information collected or maintained by or on behalf of the City and all information assets used or operated by the City, a City contractor, a City vendor, or any other organization on behalf of the City
- All IT-related directives standards and procedures required to protect information technology systems, procured with City funds, residing on City property and/or used in the conduct of City business

Policy Applies To

☒ External & Internal Applicants	☒ Temporary Employees
☒ Full-Time Employees	☒ Volunteers
☒ Part-Time Employees	☒ Grant-Funded Employees
☒ Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors and Other Third Parties

Definitions

COSA	The City of San Antonio, its departments and/or agencies.
Confidentiality	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.

Integrity	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.
Information Security Program	A framework designed to provide reasonable assurance that risk-based system and application security controls and/or countermeasures are commensurate with the value of the asset(s) they protect; are in place and working as intended to protect City information asset(s).
User	Any employee or non-employee who uses COSA-administered information assets and/or system(s), exclusive of COSA's web pages.

Information Security Management Program

The COSA Security Management Program Framework is designed to create a continuous cycle for assessing and validating risk by developing and implementing entity wide security policies and procedures as well as monitoring and periodically testing their effectiveness. Assessing and validating risk defines the management, operational, and/or technical controls necessary to protect COSA asset(s). Security Management includes risk-based countermeasures and safeguards as well as preventative, detective, and corrective security controls over remote and local access, contingency and backup planning, change and log management, cryptography, network security, patch and configuration management, physical access, and secure system development among other controls.

COSA information assets represent a significant investment by the City. As such, all City information assets must be protected from unauthorized access, use, disclosure, duplication, modification, diversion, and/or destruction whether accidental or intentional. Access to all City, non-public, information assets must be limited to what is necessary for the performance of required business tasks.

COSA's City-wide security program includes (at a minimum):

1. Periodic risk and vulnerability assessments, security evaluation and testing as well as continuous monitoring that validate risk and internal control effectiveness.
2. Coordinating development and distribution of security standards and procedures to reasonably assure cost-effective risk reduction and compliance.
3. Subordinate information security plans for networks, facilities, systems and software among other plans.
4. An annual Third-Party penetration test of externally facing COSA servers.
5. Security awareness training for City employees, contractors, officials and other third parties as well as planning and coordinating security-related activities within COSA.
6. Periodic testing and evaluation that includes testing of major risk-based systems on the COSA network as well as providing results to senior management on policy and control.
7. Maintaining a remedial action process to address deficiencies.
8. Monitoring vendor activity to help ensure compliance with the COSA security program requirements.
9. Coordinating Security Incident Response activities for detecting, reporting and/or responding to incidents.
10. Maintaining continuity of mission-essential systems including operational and contingency plans.

11. Representing COSA in the security community.

Roles & Responsibilities

Department System/Application Owners	1. System/application owners are responsible for defining security-related business requirements. 2. City departments who work with third-party users are responsible for identifying the third-party users to ITSD. 3. A System Security Plan and final security review must be approved by the system/application owner, Chief Security Officer (CSO) and the Chief Technology Officer (CTO), or their respective designees, before a being placed into production. 4. The system/application maintenance process shall include reviews of security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations. 5. Documentation shall be maintained by the system/application owner and be available to ITSD. 6. Maintain continuity of mission-essential systems including operational contingency plans. 7. All software applications obtained, purchased, leased, or developed will be through the ITSD governance and/or procurement process and provide appropriate security controls to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources.

ITSD	1. Organizational responsibility for the development, implementation, maintenance, and/or compliance monitoring of this directive is placed with ITSD. 2. ITSD Security Personnel shall have sufficient authority, training and resources to: a. Obtain data needed to monitor compliance with directives, policies/standards and procedures. b. Establish an IT and Physical Security Awareness Program. c. Execute responsibilities including staff and tools 3. ITSD Security, Project Manager Personnel & system/application owner will develop System Security Plan to ensure system/application security is addressed and documented throughout the procurement process and/or development lifecycle. 4. ITSD is responsible for publishing and disseminating the policies/standards and procedures established in this directive to all relevant personnel, third-party users including (contractors, consultants, vendors, business partners etc.). 5. Support the system/application maintenance process reviews for security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.